# クルマのソフトウェア化に伴う セキュリティ要件と求められる対応

＠日本におけるサプライチェーンとSBOMのこれから

2023/8/25

一般社団法人 Japan Automotive ISAC
技術委員会 委員長　山 﨑 雅 史（マツダ株式会社）

# AGENDA

0. 自己紹介
1. SDVを取り巻く「規制・標準」の動向
2. 継続的サイバーセキュリティ活動の必要性
3. 終わりに

# J-Auto-ISACとは？

## 情報セキュリティはチーム活動

J-Auto-ISAC Japan Automotive Information Sharing and Analysis Center

## 一般社団法人　Japan Automotive ISAC

### ＜設立の目的＞

わが国の自動車および関連するサービスを安全かつ安心に利用できるよう、サイバーセキュリティリスクのタイムリーな情報共有・分析の実現、及びサイバーセキュリティ対応能力の強化を推進する。

### ＜設立＞

2021年02月　　一般社団法人Japan Automotive ISACを設立
（会員数：111社_2023年5月末時点）

お問い合わせ先：　info@j-auto-isac.or.jp

HP：　https://j-auto-isac.or.jp/

# J-Auto-ISACとは？

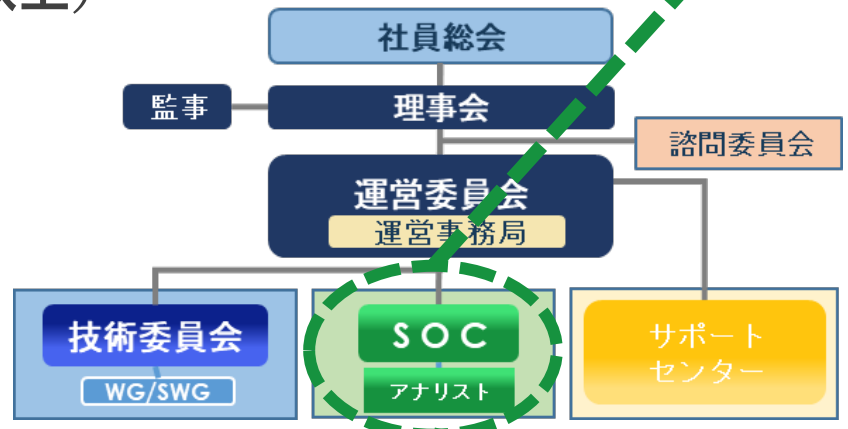
## J-Auto-ISACの提供サービスと活動内容

### SOC（Security Operation Center)

・車両や車載製品に関わる脅威・脆弱性情報の収集・分析し、DBを介して会員各社へ定期配信

・緊急度の高い情報はフラッシュレポートとして配信

・月次で分析レポートのアナリスト説明会を実施（プラチナ会員以上）




**SOC**

**インシデント情報共有**

**情報収集/分析・配信**

・以下の関連情報を適宜配信
脅威・脆弱性情報/ダークWeb情報
業界動向情報/公開脆弱性情報

**情報収集源Update**

**定期レポート**

・4半期に1回発行

**データバンク**

・データ保管/検索
・ポータルサイト

注）会員ごとに、提供されるレポート、DB閲覧に必要なIDの発行数が異なります。

# J-Auto-ISACとは？

## J-Auto-ISACの提供サービスと活動内容

### 技術委員会(WG&SWG活動)

- 会員企業で構成された３つのWGと、傘下にあるSWGで構成
- WG活動による情報共有・技術分析・意見交換を毎月実施
- テーマにより、タスクフォース等の柔軟な設置により課題解決を図ります。


**技術委員会**

**情報共有WG**
- インシデント事例検証SWG
- 脆弱性対応SWG
- グローバル連携SWG

**スキルアップWG**
- セキュリティ人材育成SWG
- 協同演習SWG
- 個別研修SWG
- ベストプラクティス策定SWG

**課題抽出・解決推進WG**
- サプライチェーンリスク対応SWG
- 情報共有プラットフォームSWG
- フォレンジック検討SWG
- SBOM-SWG

# AGENDA

0. 自己紹介
1. **SDVを取り巻く「規制・標準」の動向**
2. 継続的サイバーセキュリティ活動の必要性
3. 終わりに

# SDVを取り巻く「規制・標準」の動向

## 法規、及び標準規格やガイドラインの動き

| | | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 | 2025 | 2026 |
|---|---|---|---|---|---|---|---|---|---|---|
| サイバーセキュリティ（CS）※3 & ソフトウェア更新（SU）※3 ＜OTAを含む＞※4 | 法規 | 国連 WP29 CS/OTA TFで法規検討 | | UN ‘20/6 国連法採択 | | | 2022/7 EU適用開始 | | 2024/7 継続車 適用開始 | |
| | | | ‘20/4 自動運行車 適用開始 | | ‘20/11： 特定改造等の 許可制度 | | ‘22/7: 新型車適用 （ＯＴＡ付） | ‘24/1 新型車適用 (OTA無) | | ‘26/5 全継続車 適用 |
| | 標準 | CS（ISO21434） | | | ISO ’21/8 発行 ISO/SAE 21434:2021 | | | | | |
| | | SU（ISO24089） | | | | | ISO ’22/2 発行 ISO 24089 | | | |
| 自動運転関係 | ガイドライン | ● Federal Automated Vehicles Policy<br>● Cybersecurity Best Practices for Modern Vehicles | | | | | | | | |
| | | NHTSA 2016年版でOTAによる セキュリティパッチ配信を推奨 | | NHTSA アップデート版 （’21/1パブコメ） | | NHTSA ‘22/9 アップデート版リリース | | | | |

※3: CS: Cyber Security / SU: Software Update　※4: OTA: Over The Air update

# SDVを取り巻く「規制・標準」の動向

## UN-R155 サイバーセキュリティ法規

【業務管理システム】

| Cyber Security Management System（CSMS） | |
|---|---|
| 組織とリスクの管理 | サイバーセキュリティ管理を組織的に行うプロセスを有する |
| | 車両設計におけるサイバーセキュリティリスクを特定し、アセスメント・分類化・処置を行う |
| | テストを含め、リスクの適切な管理を確認する |
| | リスクアセスメントが最新の状態に保たれていることを確認する |
| モニタリングと攻撃・脆弱性の管理 | サイバー攻撃をモニタリングし、効果的に対応する新たな攻撃・脆弱性に照らして既存対策を評価する |
| | 成功又は未遂に終わった攻撃の分析を支援する |
| | 攻撃・脆弱性を合理的な期間内に軽減する |
| | 車両データ検知・分析等、モニタリングを継続する |
| 各要件に対して、サプライチェーンを管理する | |

【型式認定】

| Type Approval |
|---|
| CSMSが導入され、走行車両に適用可能であること |
| リスクアセスメントによる分析を行い、何がクリティカルか特定すること |
| 特定されたリスクを軽減するため、緩和策を有すること |
| 緩和策が意図通り機能するか、テストを行ってエビデンスを得ること |
| サイバー攻撃を検知し防御する手段を有すること |
| データフォレンジックを支援する手段を有すること |
| 車両型式に特化したモニタリングを実施すること |
| モニタリングの報告書を関連する当局に送付すること |

# SDVを取り巻く「規制・標準」の動向

## UN-R156　ソフトウェアアップデート法規

【業務管理システム】

| Software Update Management System(SUMS) | |
|---|---|
| ソフト・ハードとVINのトレーサビリティ管理 | 車両型式に関連したハードウェアとソフトウェアのバージョンを記録する |
| | 装置のソフトウェアがあるべき状態であることを確認する |
| | 特にソフトウェア更新に関して相互依存性を特定する |
| | 対象車両を特定し、更新の互換性を検証する |
| 法規適合性の管理 | 型式認証に関係するソフトウェアを特定する |
| | ソフトウェアの更新が型式認可や法的に定義されたパラメータに影響をあたえるかどうかを評価する（機能の追加や削除を含む） |
| ソフトウェア更新が安全性や安全運転に影響を与えるか評価する | |
| 車両の所有者に更新情報を通知する | |
| これら以上のことの記録を残す | |

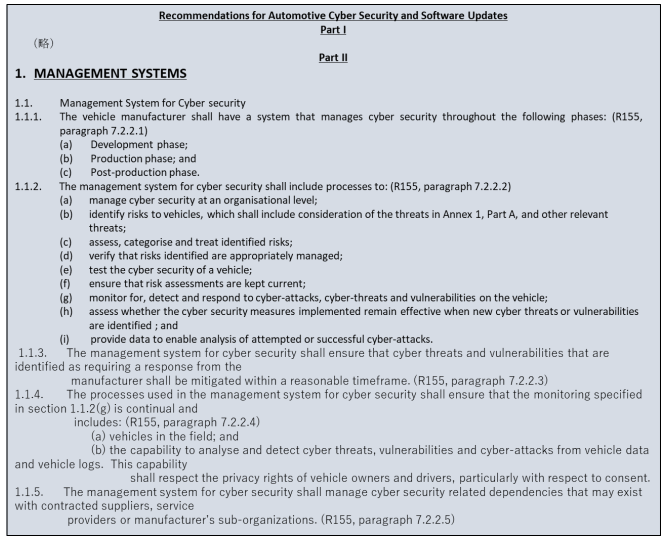
【型式認定】

| Type Approval |
|---|
| SUMSが導入され、走行車両に適用可能であること |
| SU配信機能を保護し、完全性と真正性を保証すること |
| ソフトウェア識別番号を保護すること |
| ソフトウェア識別番号が車両から読み出せること |
| OTAは以下の要件を満たすこと |
| 　更新に失敗した場合のリストア機能を有すること |
| 　十分な電源がある場合のみに更新を実行すること |
| 　安全な実施を保証すること |
| 　各更新と完了についてユーザーに通知すること |
| 　車両が更新実施が受入可能なことを保証すること |
| 　整備士が必要なときにユーザーに通知すること |

# SDVを取り巻く「規制・標準」の動向

## 各国の規制動向：国連1998年協定※加入国

- GTRではなく先ずはTechnical Requirement （TR）を策定し、2022年９月にGRVAへ提出済
- GTR化は今後、検討の見込み



Recommendations for Automotive Cyber Security and Software Updates

Part I

（略）

Part II

**1. MANAGEMENT SYSTEMS**

1.1. Management System for Cyber security

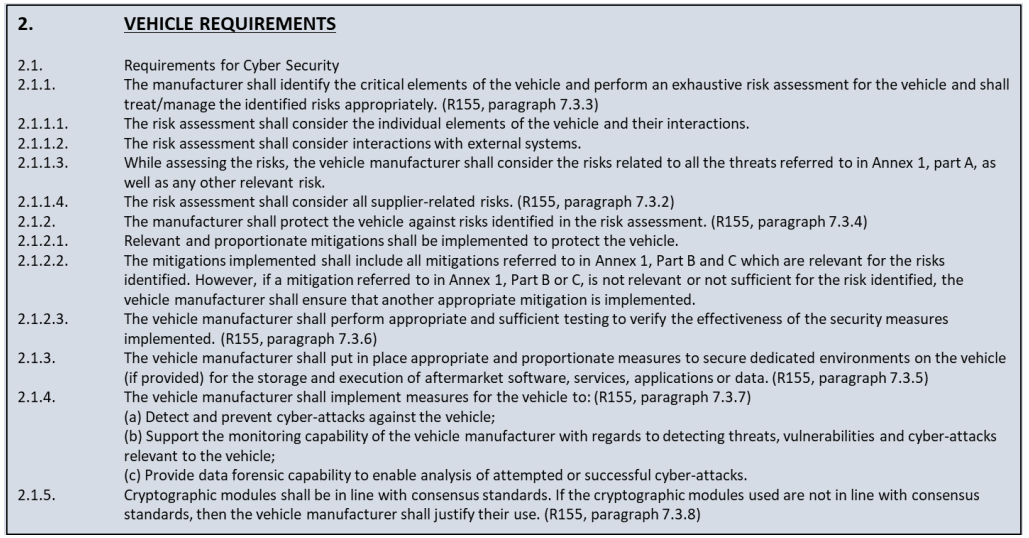
1.1.1. The vehicle manufacturer shall have a system that manages cyber security throughout the following phases: (R155, paragraph 7.2.2.1)
- (a) Development phase;
- (b) Production phase; and
- (c) Post-production phase.

1.1.2. The management system for cyber security shall include processes to: (R155, paragraph 7.2.2.2)
- (a) manage cyber security at an organisational level;
- (b) identify risks to vehicles, which shall include consideration of the threats in Annex 1, Part A, and other relevant threats;
- (c) assess, categorise and treat identified risks;
- (d) verify that risks identified are appropriately managed;
- (e) test the cyber security of a vehicle;
- (f) ensure that risk assessments are kept current;
- (g) monitor for, detect and respond to cyber-attacks, cyber-threats and vulnerabilities on the vehicle;
- (h) assess whether the cyber security measures implemented remain effective when new cyber threats or vulnerabilities are identified ; and
- (i) provide data to enable analysis of attempted or successful cyber-attacks.

1.1.3. The management system for cyber security shall ensure that cyber threats and vulnerabilities that are identified as requiring a response from the manufacturer shall be mitigated within a reasonable timeframe. (R155, paragraph 7.2.2.3)

1.1.4. The processes used in the management system for cyber security shall ensure that the monitoring specified in section 1.1.2(g) is continual and includes: (R155, paragraph 7.2.2.4)
- (a) vehicles in the field; and
- (b) the capability to analyse and detect cyber threats, vulnerabilities and cyber-attacks from vehicle data and vehicle logs. This capability shall respect the privacy rights of vehicle owners and drivers, particularly with respect to consent.

1.1.5. The management system for cyber security shall manage cyber security related dependencies that may exist with contracted suppliers, service providers or manufacturer's sub-organizations. (R155, paragraph 7.2.2.5)



**2. VEHICLE REQUIREMENTS**

2.1. Requirements for Cyber Security

2.1.1. The manufacturer shall identify the critical elements of the vehicle and perform an exhaustive risk assessment for the vehicle and shall treat/manage the identified risks appropriately. (R155, paragraph 7.3.3)

2.1.1.1. The risk assessment shall consider the individual elements of the vehicle and their interactions.

2.1.1.2. The risk assessment shall consider interactions with external systems.

2.1.1.3. While assessing the risks, the vehicle manufacturer shall consider the risks related to all the threats referred to in Annex 1, part A, as well as any other relevant risk.

2.1.1.4. The risk assessment shall consider all supplier-related risks. (R155, paragraph 7.3.2)

2.1.2. The manufacturer shall protect the vehicle against risks identified in the risk assessment. (R155, paragraph 7.3.4)

2.1.2.1. Relevant and proportionate mitigations shall be implemented to protect the vehicle.

2.1.2.2. The mitigations implemented shall include all mitigations referred to in Annex 1, Part B and C which are relevant for the risks identified. However, if a mitigation referred to in Annex 1, Part B or C, is not relevant or not sufficient for the risk identified, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented.

2.1.2.3. The vehicle manufacturer shall perform appropriate and sufficient testing to verify the effectiveness of the security measures implemented. (R155, paragraph 7.3.6)

2.1.3. The vehicle manufacturer shall put in place appropriate and proportionate measures to secure dedicated environments on the vehicle (if provided) for the storage and execution of aftermarket software, services, applications or data. (R155, paragraph 7.3.5)

2.1.4. The vehicle manufacturer shall implement measures for the vehicle to: (R155, paragraph 7.3.7)
(a) Detect and prevent cyber-attacks against the vehicle;
(b) Support the monitoring capability of the vehicle manufacturer with regards to detecting threats, vulnerabilities and cyber-attacks relevant to the vehicle;
(c) Provide data forensic capability to enable analysis of attempted or successful cyber-attacks.

2.1.5. Cryptographic modules shall be in line with consensus standards. If the cryptographic modules used are not in line with consensus standards, then the vehicle manufacturer shall justify their use. (R155, paragraph 7.3.8)

※1998年協定加入国
　1958年協定に加入できなかった米国を考慮し、日米欧のイニシアティブで成立。アジアからは、日本、中国、インド、韓国、マレーシアが加入

# SDVを取り巻く「規制・標準」の動向

## 各国の規制動向

【英国】
　判例法から成っているため、国連法規（UN-R155, 156）を要求する記載は未だないが、EU離脱後に法整備を進めており近々、リリースされる事が予想される

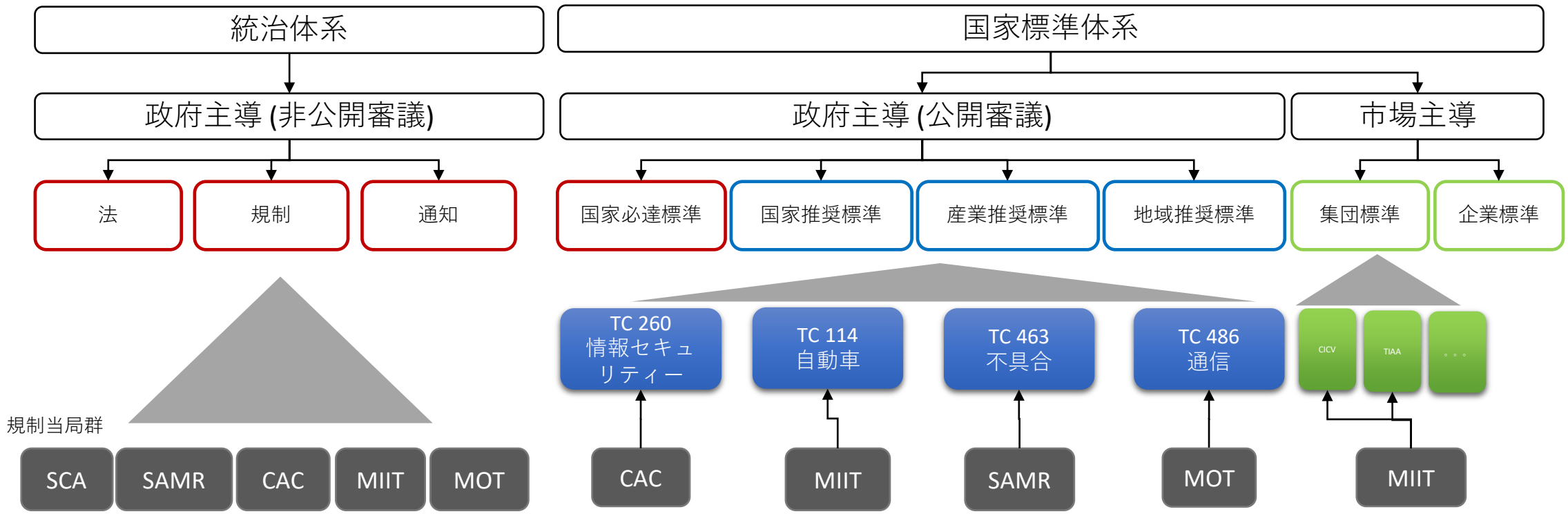
【インド】
　UN-R155 をコピペした「規格DRAFT」を策定中
　対象、実施について現時点は情報無し

【韓国】
　５８協定国でもあるが、型式認証は無い
　　2020年　ガイドラインをリリース
　　2021年7月　法案（MotorVehicleControlAct)発表

# SDVを取り巻く「規制・標準」の動向

## 各国の規制動向：中国

### 電動車を筆頭に独自ガイドラインを大量に発行




**赤枠:** 遵守が必須
**国家必達標準：** ベースライン要求
**青枠（推奨標準）：** 市場要求におけるベストプラクティス
**緑枠（集団 / 企業標準）：** 左に並ぶ標準類に比べると高水準の要求

**MIIT:** Ministry of Industry and Information Technology, 工业和信息化部
**MOT:** Ministry of Transport，交通运输部
**SAMR:** State Administration for Market Regulation，市场监督管理局
**CAC:** Cyberspace Administration of China，国家互联网信息办公室
**SCA:** National Cryptography Administration 国家密码管理局

# SDVを取り巻く「規制・標準」の動向

## 関連規制動向（車両データに関する規制）

【ＥＵ】

車両内データ利活用：欧州ではEU競争力の獲得に向け「EU域内の全産業を横断したデータ利活用」を推進する「EUデータ法」の法案が出されており’23年末までに可決される見込み。利活用に向けてデータ内容と通信方式をどこまで規制対象とするかが論点となっている。

【中国】

国家安全保障の観点から、データ分野に関する規制を強化

＜法体系＞

青字:施行済みの法令　赤字:直近施行の法令　黒字:意見募集稿の段階

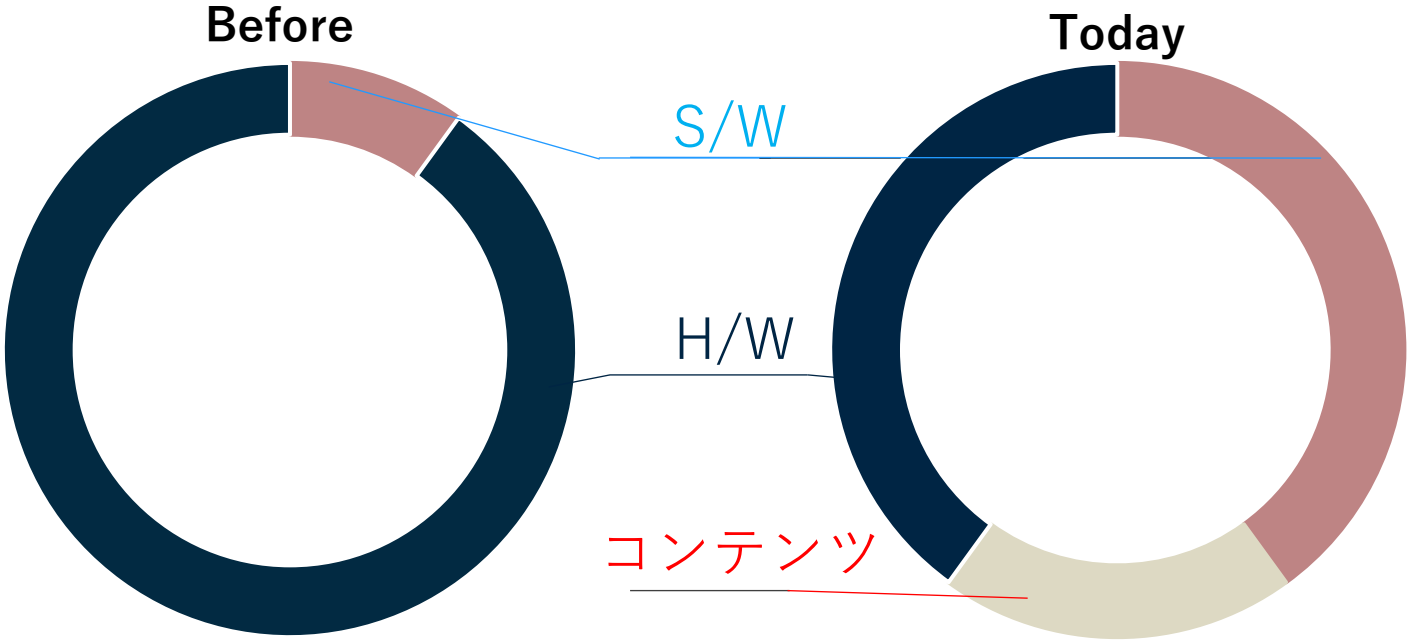
| | | | | |
|---|---|---|---|---|
| 目的・対象 | | データセキュリティ（国家核心データ／重要データ） | ネットワークセキュリティ | 個人情報の保護 |
| 法律 | | ①データ安全法（21年6月公布、9月施行） | サイバーセキュリティ法（17年6月施行） | ③個人情報保護法（21年8月公布、11月施行） |
| 細則 | 全国レベル | •データ安全管理弁法 (意見募集稿)<br>•データ越境安全評価ガイドライン (意見募集稿)　等 | •サイバーセキュリティ等級保護基本要求<br>•サイバーセキュリティ等級保護等級決定ガイドライン　等 | •個人情報安全規範<br>•個人情報越境移転安全評価弁法 (意見募集稿)　等 |
| | 業界レベル | ②自動車データ安全管理規定（21年8月公布、10月施行）　等 | | |

# AGENDA

0. 自己紹介
1. SDVを取り巻く「規制・標準」の動向
2. **継続的サイバーセキュリティ活動の必要性**
3. 終わりに

# 継続的サイバーセキュリティ活動の必要性

## SDVはサプライチェンを構成するプレーヤーも大きく変化




主にOEMやTier1 が提供
- ボディ
- パワートレイン
- 電装系
- シート
- コンポーネント & HMI

多くの企業が参加
- OEM
- サプライヤ
- OSベンダー
- チップベンダー
- ISP、ISV
- In-car-アプリ

- **エンターテイメント**
  音楽、ビデオなどのコンテンツ配信サービス
- **ソーシャルメディア**
  Facebook, LineなどSNSサービスへの接続
- **カーシェアリング**
  所有から、サービスへの移行
- **Points of interest**
  スポンサード情報を含む目的地提案
- **福祉サービス**
  自動運転によるデイケア、過疎地の移動手段提供
- **テレマティックス保険**
  ドライバや運転タイプによる保険料の最適化
- **緊急連絡、自動停車、自動搬送**
  ドライバーの異変などの緊急時に車両が自動対応
- **盗難防止**
  盗難にあった車両の位置情報を通知し、遠隔操作

※1:CASE：Connected, Autonomous, Shared, Electric

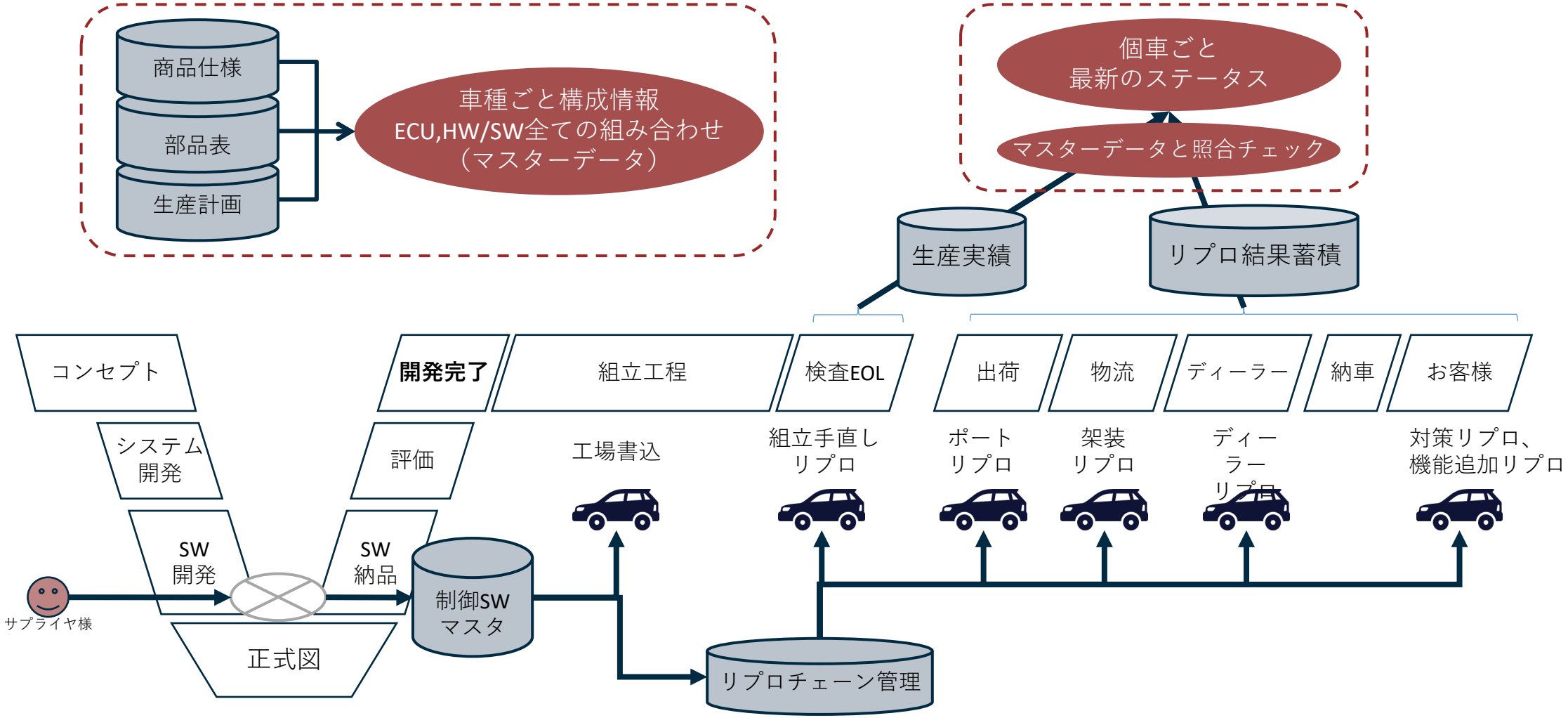
# 継続的サイバーセキュリティ活動の必要性

## SDVのセキュリティ脅威・インシデントは多種・多様

| 分類 | | 脅威・攻撃 | 影響・損害の可能性 | インシデント事例 |
|---|---|---|---|---|
| 制御系 | 安全系 | ・ブレーキ、ハンドル操作、エンジンなどに対する不正な制御<br>・走行制御ロジックの改ざん<br>・センサーデータ改ざん | 人命に係るセーフティへの侵害 | テレマテクス装置TCU Dongleの脆弱性悪用 |
| | | | リコールによる経済的損失 | クライスラーUconnect脆弱性 140万台リコール |
| | 安全以外 | ・ドアロック不正操作、エンジン始動 | 自動車盗難 | イモビライザー解除ツール |
| | | ・ワイパー不正操作、その他ボディ系不正操作 | 意図しない動作による不安感の誘発 | クライスラーUconnect脆弱性悪用 |
| | | | バッテリー上がり、電力消費 | ― |
| 情報系 | 情報窃取 | ・任意の情報操作コマンドの実行 | 任意の情報の外部送信、詐欺被害 | GMテレマティクスOnStar RemoteLink アプリの脆弱性 |
| | | ・ドライブレコーダログ情報改ざん、DoS攻撃 | 保険、情報サービスの妨害 | 自動車遠隔管理サーバへの不正ログイン |
| | その他、プライバシー侵害等 | ・位置情報、車両情報、運転履歴情報、個人情報の漏えい<br>・クラウド系攻撃 | プライバシー侵害 | 無線ネット技術の漏えい |
| | | ・その他通信情報の盗聴 | 情報漏えい | 車車間WLAN 802.11pの盗聴 |

# 継続的サイバーセキュリティ活動の必要性

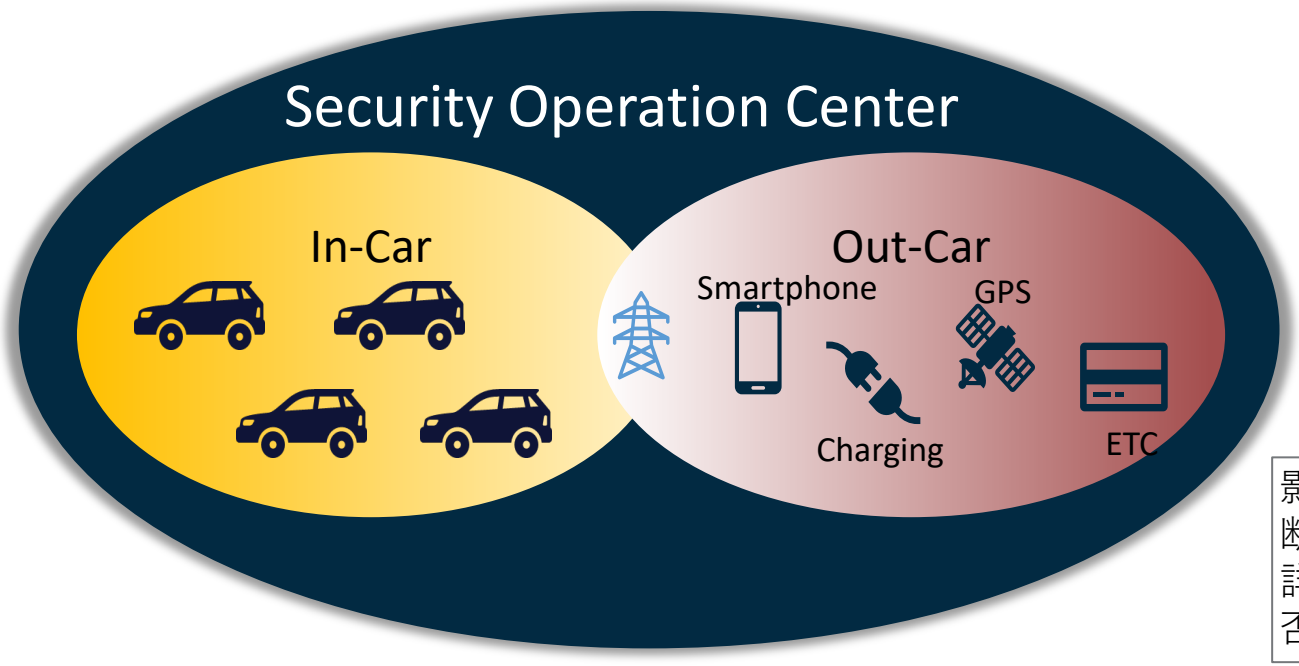
法規を満足した上で、リスクへの対応を確実に行っていく為には・・・

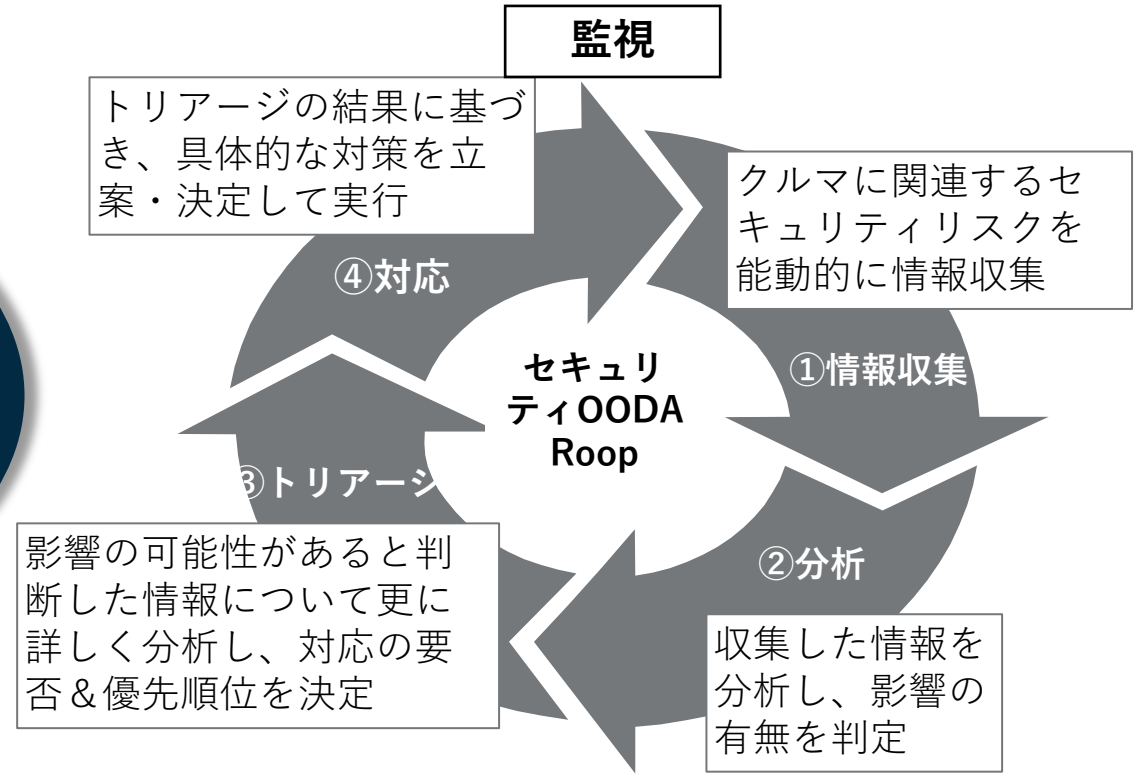



ライフサイクルに渡って「トレーサビリティ管理」の実施が必要

# 継続的サイバーセキュリティ活動の必要性

## In-Car/Out-Car含めたセキュリティ品質保証

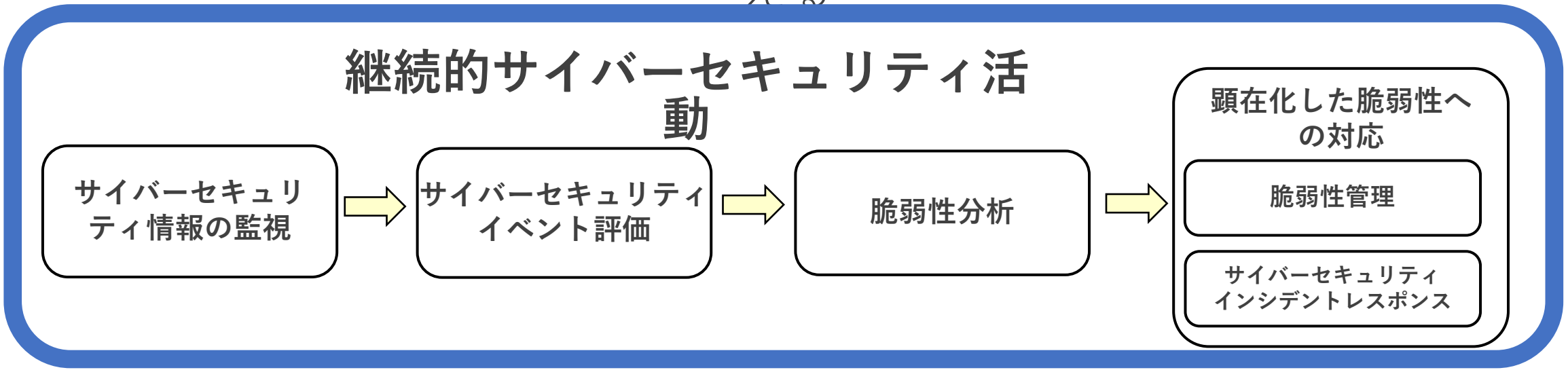



ライフサイクルに渡っての脅威・脆弱性ハンドリングは必須

# 継続的サイバーセキュリティ活動の必要性

これまでのクルマの品質保証の仕組みに継続的サイバーセキュリティ活動を加える

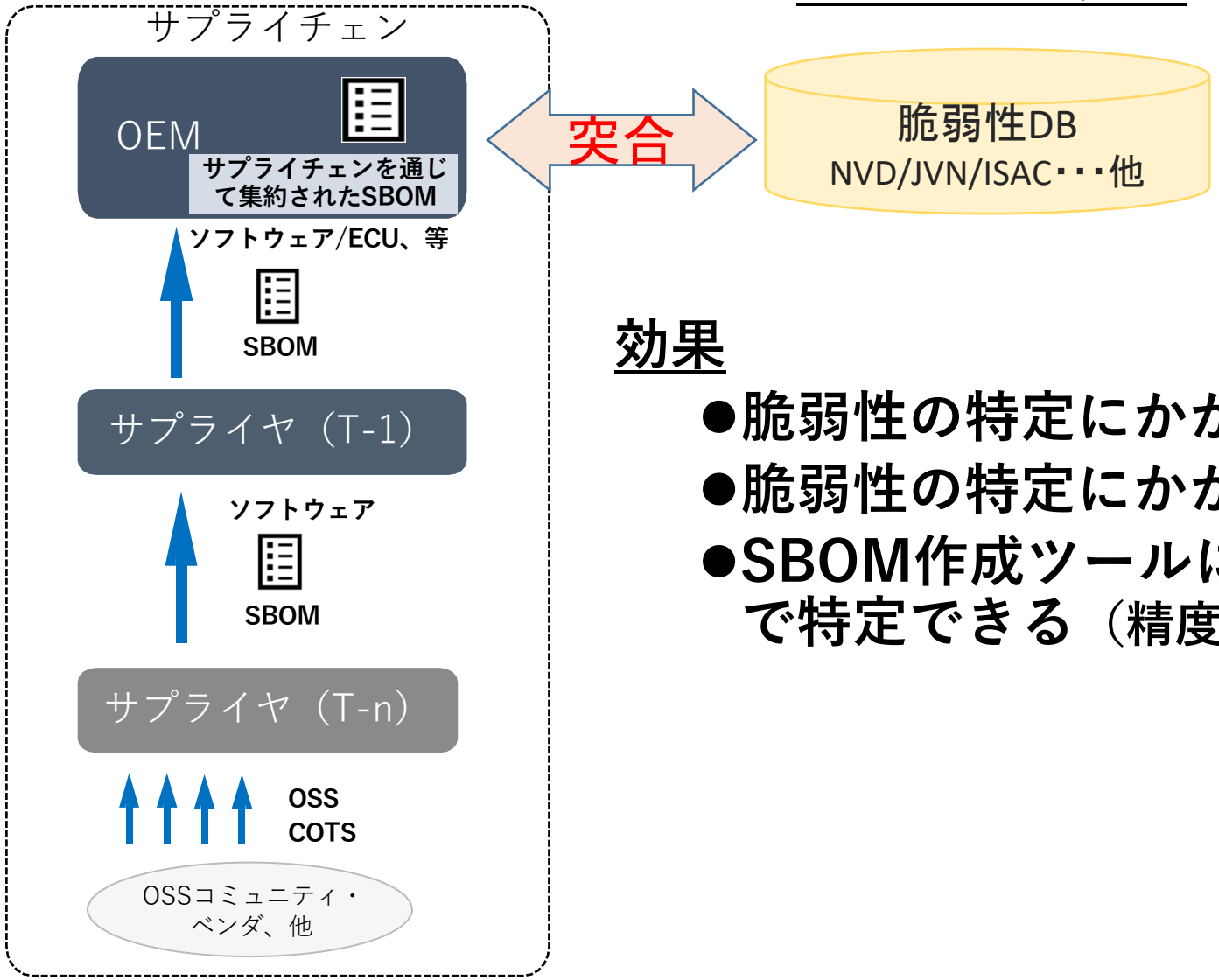



## これまでのクルマの品質保証の仕組み

設計検証　不具合解析　市場対応

# 継続的サイバーセキュリティ活動の必要性

## SBOMの活用




**効果**

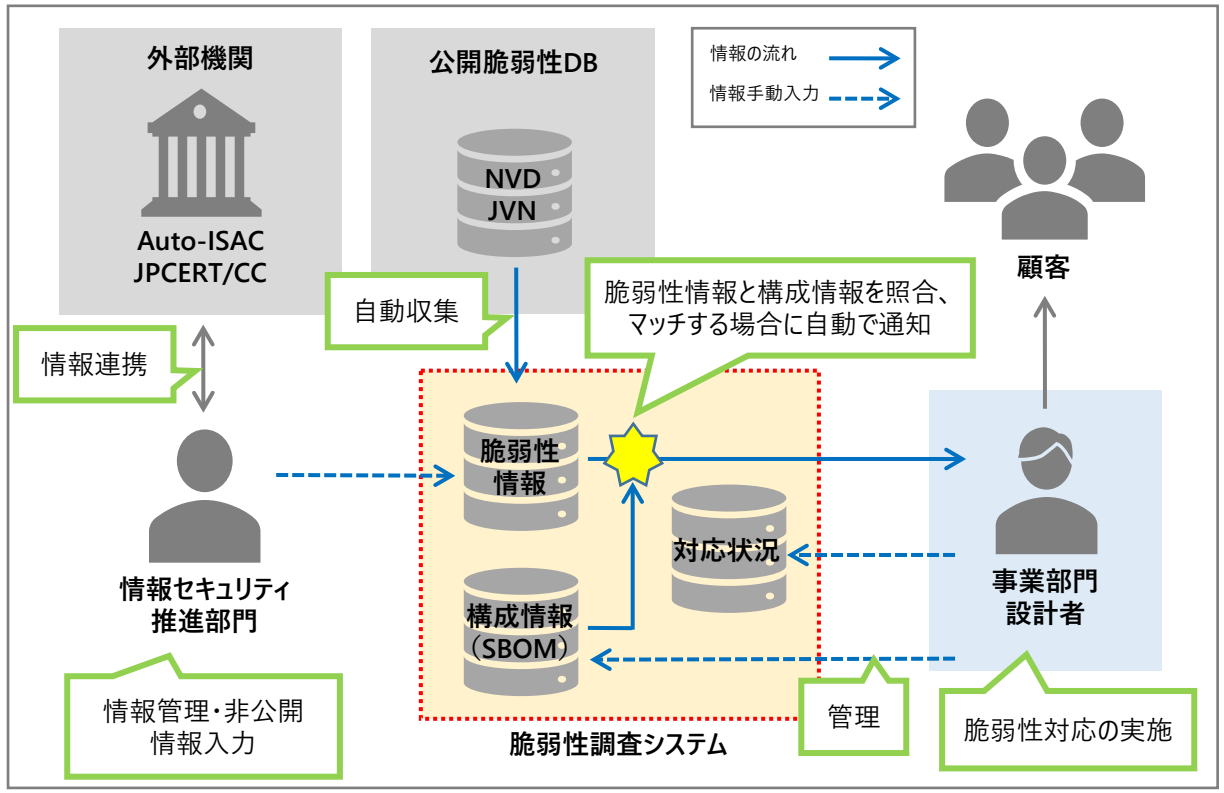
- **脆弱性の特定にかかるコストが削減する**
- **脆弱性の特定にかかるリードタイムが短縮する**
- **SBOM作成ツールによっては、OSSが使用するOSSまで特定できる（精度向上）**

# 継続的サイバーセキュリティ活動の必要性

## 自動車業界におけるSBOM活用事例

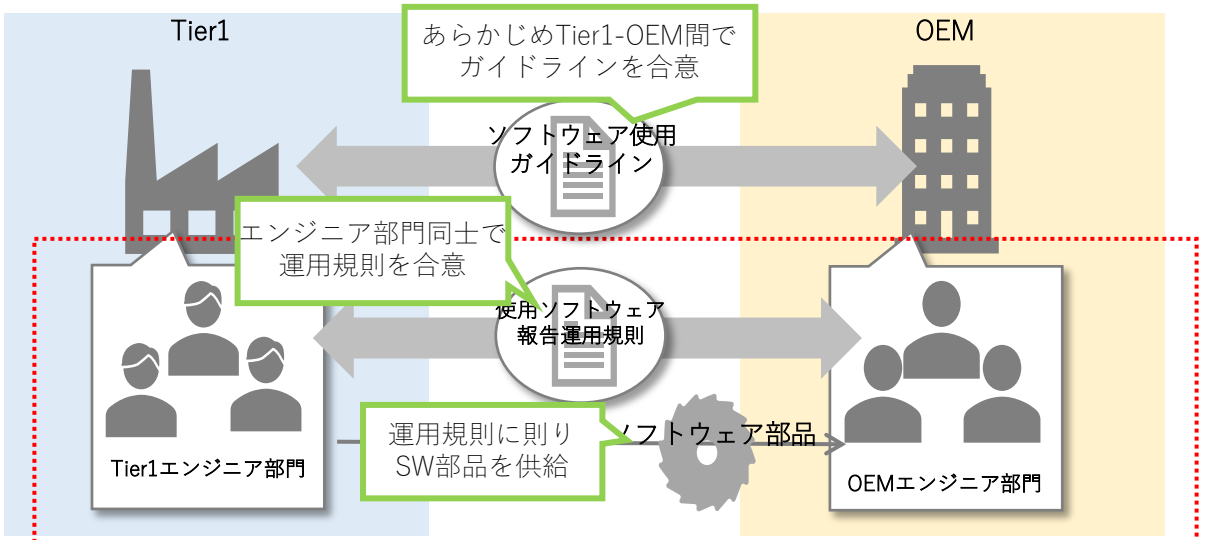
SBOM作成主体
SBOM活用主体

### 事例１： 脆弱性調査システムを用いた脆弱性対応




### 事例２： ライセンス規約準拠におけるSBOMの活用

| | | |
|---|---|---|
| ガイドライン(会社間のベーシックなルールの合意) | • サプライチェーンにおけるOSSコンプライアンスの役割<br>• 責任分界 | • 各ライセンスの取扱い<br>• 使用ソフトウェアリスト提供の合意 |
| 運用規則(実務レベルの運用ルールの合意) | • SBOMフォーマット<br>• ワークフロー | • 報告のタイミング<br>• 連絡先 |

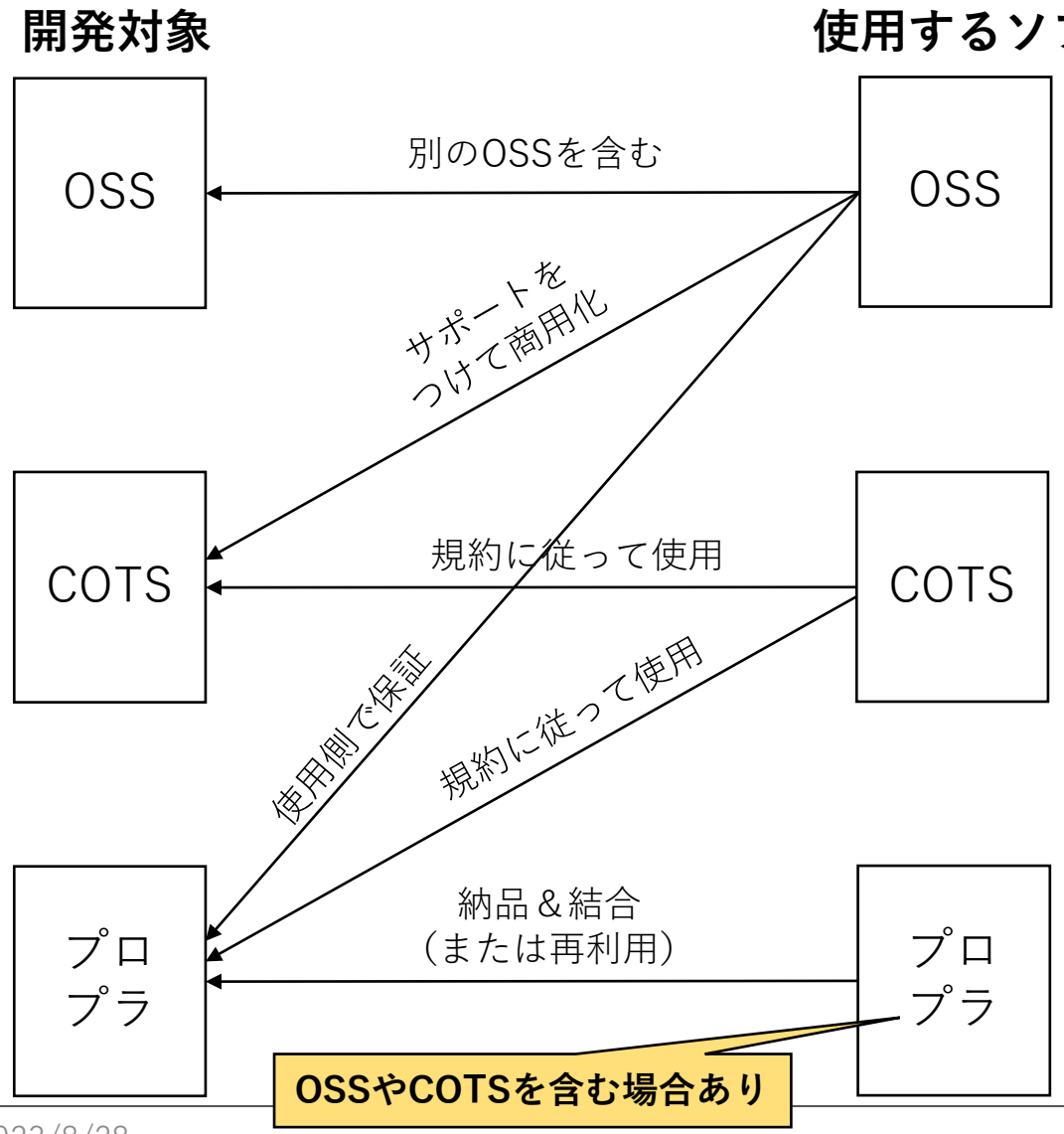



**SBOMの活用は先進企業の一部にまだまだ限られている**

出展：経済産業省　OSS の利活用及びそのセキュリティ確保に向けた 管理手法に関する事例集,

# 継続的サイバーセキュリティ活動の必要性

## SBOMで扱うクルマのソフトウェアの種別と関係

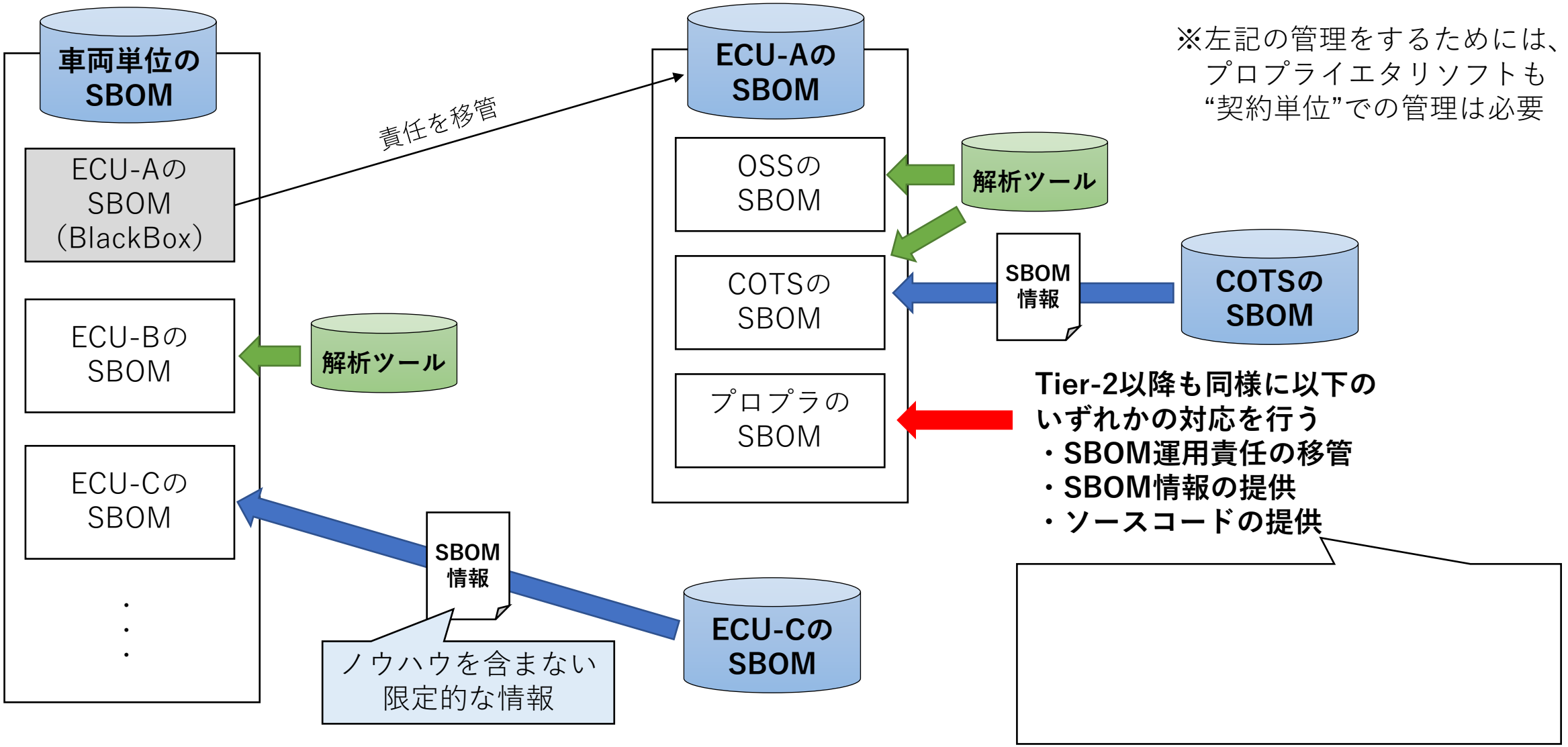



- OSS、COTS、プロプライエタリソフトの３種類が挙がっているが「開発する対象」と「使用するソフトウェア」の区別が必要
- OSSはSBOMに登録するが、OSSの開発者がSBOM情報を提供してくれるとは限らない
- 車載ソフトは、最終的にプロプライエタリソフトになるため、SBOMへの登録は必要
  （UN-R156で管理するRXSWINとの関連付けも可能）

- これらの関係性を踏まえた上で、SBOMの利用方法を検討する必要がある

# 継続的サイバーセキュリティ活動の必要性

## SBOMの運用責任は？



# 継続的サイバーセキュリティ活動の必要性

## 自動車業界におけるSBOM活用における課題

**課題**

- CSMS／SUMSはOEMが担保する責務を持っており、クルマやシステム（ソフトウェアを含む）を相互に供給するケースも同様だが業界として共通の効果的なSBOMの作成者や対象範囲が不明
- SBOMの項目、粒度、フォーマッ ト、部品命名規則等が標準化されていない
- 契約、責任、費用負担が整理されていない
- SBOM作成ツールの導入コスト低減とツール自体の機能および精度向上が必要
- グローバルサプライチェーンにおいて国内外の基準の整合が必要

# 継続的サイバーセキュリティ活動の必要性

## 課題解決に向けたJ-Auto-ISACの活動計画

| 活動 | | 2023年 4月 | 5月 | 6月 | 7月 | 8月 | 9月 | 10月 | 11月 | 12月 | 2024年 1月 | 2月 | 3月S |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SWG定例会 | | ◆4/20 #1 | ◆5/18 #2 | ◆6/15 #3 | ◆7/20 #4 | ◆8/17 #5 | ◆9/21 #6 | ◆10/19 #7 | ◆11/16 #8 | ◆12/21 #9 | ◆1/18 #10 | ◆2/15 #11 | ◆3/21 - #12 |
| 活動の流れ | | ガイドライン作成（初版） | | | | | | | | 普及計画作成 | | 次年度準備 | |
| 計画策定 | 各社課題を基にガイドラインのスコープを定め、検討論点、要調査項目、計画を決定 | 意見募集 | 日程・スコープ決定 | 要調査項目 | | | | | | | | | |
| 事前調査 | 文献調査、外部団体への聞き取り調査（発行物、関連組織・団体、業界動向） | | | 初期調査 | | | 追加調査① | | | 追加調査② | | | |
| 外部連携 | ガイドラインへの意見募集、事前レビュー<br>※他業界との足並みを揃える為 | 意見募集 | 意見 | | 調査結果 | | 調査結果 | レビュー | | | | | |
| 文書作成 | 調査結果よりガイドラインのコンテンツを検討し、骨子作成→詳細作成→最終化を実施 | | | スコープ再確認・骨子の作成 | | | コンテンツ詳細作成<br>協議・レビュー | | | | ガイドライン最終化 | | |
| 課題整理 | 年間を通じて蓄積された検討課題について、対応方針・優先度付の明確化 | | 課題の蓄積・管理 | | | | | | | | 棚卸 | 次年度向け課題 | |
| 次年度計画策定 | 次年度の計画を策定（ガイドライン普及計画およびSWG次年度活動計画） | | | | | | | | | 普及計画作成 | | WBS作成 | |

# ご清聴ありがとうございました！

J-Auto-ISAC
Japan Automotive Information Sharing and Analysis Center

ホームページ：　https://j-auto-isac.or.jp/

〒108-6028　東京都品川区港南2-15-1　インターシティA棟28階
一社）Japan Automotive ISAC　事務局　高木憲生（Norio Takagi）
mailto:norio.takagi@j-auto-isac.com